READINESS AND EMERGENCY MANAGEMENT FOR SCHOOLS REMS TECHNICAL ASSISTANCE CENTER

Episode 8: Successful Strategies for Addressing Cybersecurity and Cyber Safety

***#REMSontheAir* Podcast Intro (Recorded):** [00:00:00] Welcome to the *#REMSontheAir* Podcast, hosted by your partners at the U.S. Department of Education's Office of Safe and Supportive Schools and its Readiness and Emergency Management for Schools Technical Assistance Center. If you're an old friend, you know us as the REMS TA Center, your national school safety center.

Join us as we chat about key topics in school and campus safety, security, and emergency management with experts and partners from the field.

Janelle Hughes: Hello and welcome back. We are excited to host another *#REMSontheAir* Podcast. My name is Janelle Hughes. For those who may have missed the first few podcast segments, I'm the Project Director for the REMS TA Center. Today, I'm joined by my colleague, Amanda Everett, our lovely REMS TA Center Training Manager. [00:01:00]

Amanda Everett: Thanks so much, Janelle. I look forward to discussing the critical connection between cybersecurity and cyber safety because the two go hand in hand. We all know that COVID-19 dramatically increased the usage of digital learning formats, the education agencies across the nation, and, for many, shifted the learning environment to school at home.

Unfortunately, these education agencies are also being targeted deliberately by cyber actors with cyber threats, which can cause disruptions to the learning environment, as well as overall school operations. So, education officials must be aware of and prepared to address and manage these threats.

Janelle Hughes: It's so true, Amanda.

When more education agencies across the country began teaching and learning and in virtual or school at home settings during the spring of 2020, many schools moved to online platforms to conduct virtual teleconferencing or to create their virtual classrooms. [00:02:00] We saw this trend taking place across sectors, as well.

Community partners, for example, had to also rethink how to offer trainings, and many opted to host them in a virtual setting. During that time, the Federal Bureau of Investigation distributed a press release warning of online classroom hijacking and Zoom bombing, as it was known, in virtual engagement settings, including webinars and virtual meetings, during which hackers were exposing students and adults to inappropriate content.

In specific support of schools, the bulletin also included valuable prevention and mitigation activities that schools can employ to protect the whole school community online. In fact, the REMS TA Center now offers a new online course that describes this and other issues in more details. The course is called Cybersecurity Considerations for K-12 Schools and School Districts, and you can find it on our trainings page.

Amanda Everett: Thanks for sharing that resource, Janelle. There were so [00:03:00] many unknowns at the beginning of the pandemic, and many education agencies were forced to pivot to online instruction, almost overnight, not really knowing what to expect. Now, I'm sure many recognize how important it is for schools and districts to incorporate cybersecurity and safety into their existing curricula, as well as their continuity of teaching and learning planning for any emergency, and they can do this specifically through a cyber annex to their EOPs [emergency operations plans].

Janelle Hughes: Amanda, before we go any further, should we explain the difference between cybersecurity and cyber safety so that we can make sure we all have a common understanding?

Amanda Everett: Yes, good idea, Janelle. Cybersecurity deals more with the threats to a school's or school district's data, network, and systems, whereas cyber safety includes threats to people in the school community.

Cyber safety is a shared responsibility of students, parents, and school personnel, and helps to maintain a [00:04:00] safe school in all settings, in all times, including school at home and in person. Janelle, you mentioned the Zoom-bombing incidents earlier. Are there other examples of hackers infiltrating school district systems?

Janelle Hughes: Unfortunately, there are. In fact, according to the U.S. Government Accountability Office's analysis of data gathered by the K-12 Cybersecurity Resource Center, from July 2016 to May 2020, thousands of K-12 students were affected by reported data breaches that compromised their academic records, assessment scores, and special education records.

Also, records containing students' personally identifiable information, also known as PII, such as Social Security numbers, were the second most commonly compromised type of information. And it's not just student information that is compromised, but school [00:05:00] personnel records are also vulnerable to attack.

In a previous webinar that we hosted in 2014 with our partners at the U.S. Department of Education and the Department of Homeland Security, this was discussed. Here's a snippet from that webinar.

Jason Gates (Recorded): Cyber intrusions, data breaches, and attacks at K-12 schools have increased dramatically over the last decade. These incidents expose the sensitive personal information of students and staff, disrupt critical operations, and impose high financial costs sometimes. DHS offers a variety of resources, programs, and tools to help K-12 schools establish and maintain secure networks and to prevent cyberattacks.

Amanda Everett: As recently as December 2020, several Federal agencies, including the FBI, released a joint cybersecurity advisory with more threat details, reporting numerous ransomware attacks against K-12 educational institutions.

It also included action steps and best practices schools can take to [00:06:00] increase cybersecurity. The malicious cyber actors in these attacks are slowing or impeding access to school computer systems, which disrupts the learning environment for many, especially those learning at home. These cyber actors also steal and then threaten to leak confidential data to the public unless institutions pay a ransom.

And since many students are still learning virtually, they are vulnerable to more threats such as the ones you mentioned, but there may also be an increase in cyberbullying, sexting, sextortion, oversharing, and online predation. Phishing emails, text messages, and scams with COVID-19 themes have been trending, too.

The good thing is that schools can work in collaboration with their partners to be prepared. Awareness builds preparedness.

Janelle Hughes: I think we need to place that on a billboard: Awareness builds preparedness. We know there are several strategies that schools and school districts can employ to help identify, [00:07:00] protect, detect, respond, and recover from, or prepare for, cyber threats, and to prioritize cybersecurity and safety in—within school overall planning.

We've already talked about integrating a cybersecurity annex or a cyber threat- and hazard-specific annex within a school emergency operations plan, and that is truly going to be critical. The information technology department within schools, as well as other technical staff and partners can help contribute to the development and enhance school EOPs and track current cybersecurity and cyber safety trends to provide information and guidelines to school staff, teachers, students, and families. Education agencies can use filtering and blocking software to help keep cyberattackers out, and also to prevent situations where students are accessing inappropriate content.

Also, schools can develop what is referred to as a responsible use policy [00:08:00] or an acceptable use policy, similar to student codes of conduct and student handbooks used in the traditional teaching and learning setting, which are designed to provide guidance to students on behaviors and actions that are considered acceptable and unacceptable in the school setting.

These acceptable or responsible use policies may cover issues such as expectations for online behavior, personal and academic integrity when using technology, and how student data and information will be used by the school. These policies really teach students what it means to be

a responsible digital citizen—aka someone who uses appropriate responsible behavior when engaging with technology within the school community and the community, and, of course, the world at large.

Amanda Everett: These are all such great strategies. I would also add that schools and districts can incorporate digital citizenship into lesson plans to teach students about safety, privacy and security, cyberbullying and digital drama, [00:09:00] digital footprints and reputation, and overall what it means to be a responsible digital citizen.

Youth, parents, teachers, and school personnel—all have an important role to play when it comes to cyber safety, from organizing cyber safety training opportunities at school to having discussions with children about online behavior.

Janelle Hughes: We truly really all have a role to play, and the REMS TA Center is here to provide school personnel with as much information as possible to support their staff and students in this important work.

Students have an important role to play in their digital citizenship, too, by monitoring their online behavior, which can prevent a predator from accessing their personal information. Parents can talk to their children or their child about online safety, how they interact online, and their expectations of online behavior.

And, most importantly, parents must monitor what their children post [00:10:00] online. Finally, school staff and families can support students by ensuring they know they can and should report online threats to a teacher or a school counselor or a parent, a guardian, or another trusted adult. Threats can also be reported to the National Center for Missing & Exploited Children's CyberTipline by calling 1-800-843-5678.

Amanda Everett: As you mentioned, Janelle, the REMS TA Center recognizes the importance of cybersecurity and cyber safety in all settings and all times, including during the COVID-19 pandemic and after. We have created several resources for you to check out after today and have more on the way. Download and read our fact sheet on cyber safety considerations for K-12 schools and school districts to learn more about preparing for online threats to students in our TA Snapshot or cyber safety quick links for [00:11:00] protecting youth to access key practical steps and quick links to free cyber safety resources, tools, and training.

Janelle Hughes: Thank you so much for tuning in today. Remember to follow us on social media at @remstacenter and to bookmark the *#REMSontheAir* hashtag to get information on all of the resources that we'll provide around this topic and others.

If you have any questions on the things we discussed today or want to learn more, send us your questions by email at info@remstacenter.org or give us a call at 1-855-781-7367.

Amanda Everett: Don't forget that you can also email us at any time at info@remstacenter.org to join our mailing list, where you'll get up to date on webinars, Web chats, and other virtual opportunities to learn and share.

Access additional *#REMSontheAir* Podcast [00:12:00] episodes. And share this one with your colleagues by visiting the REMS TA Center's podcast page and clicking the share tabs that appear along the left side of your screen.

Our podcast page also provides access to applicable resources on the topics we covered today, including those mentioned during today's episode and more resources on other key school and campus safety, security, emergency management, and preparedness topics.